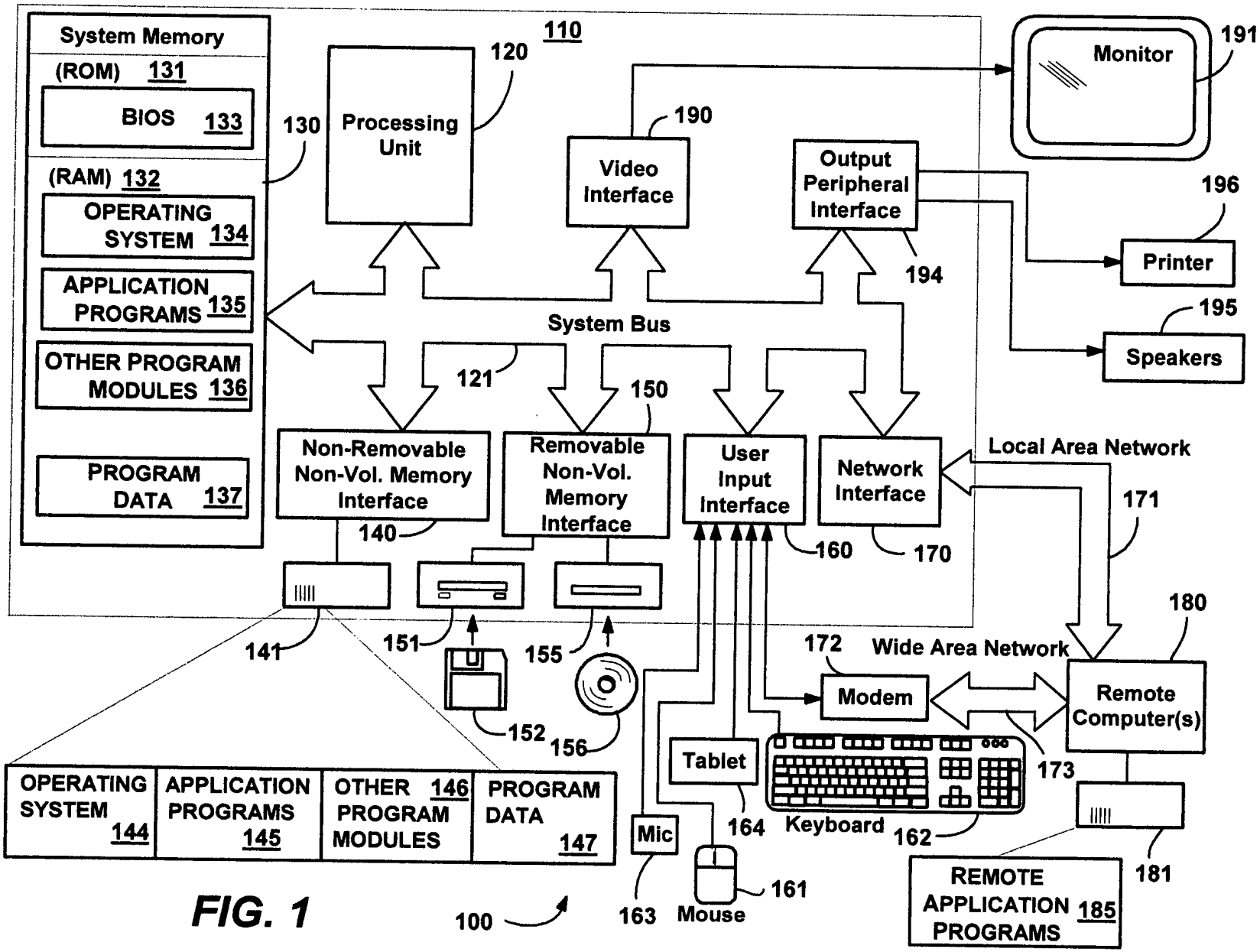

System Memory
(ROM) 131
BIOS 133
(RAM) 132
OPERATING SYSTEM 134
APPLICATION PROGRAMS 135
OTHER PROGRAM MODULES 136
PROGRAM DATA 137
130
110
Processing Unit
120
Video Interface
190
Monitor
191
Output Peripheral Interface
194
196
Printer
195
Speakers
System Bus
121
150
Non-Removable Non-Vol. Memory Interface
140
Removable Non-Vol. Memory Interface
User Input Interface
160
Network Interface
170
Local Area Network
171
180
141
151
155
172
Wide Area Network
Modem
Remote Computer(s)
152
156
Tablet
164
Keyboard
162
173
OPERATING SYSTEM 144
APPLICATION PROGRAMS 145
OTHER PROGRAM MODULES 146
PROGRAM DATA 147
Mic
163
Mouse
161
181
REMOTE APPLICATION PROGRAMS 185
100

FIG. 1

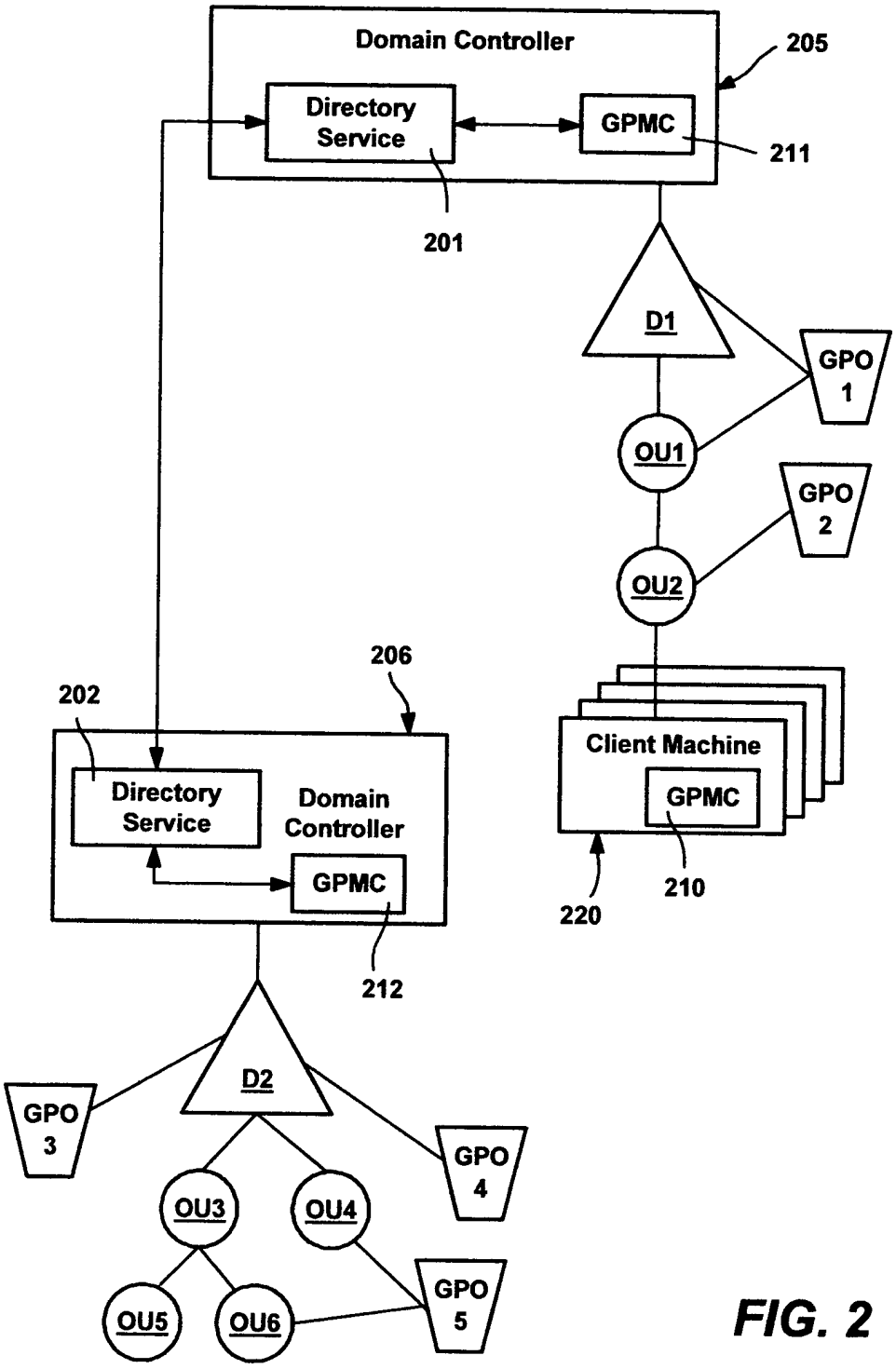

Domain Controller
205
Directory Service
GPMC
211
201
D1
GPO 1
OU1
GPO 2
OU2
206
202
Client Machine
GPMC
Directory Service
Domain Controller
GPMC
220
210
212
D2
GPO 3
GPO 4
OU3
OU4
GPO 5
OU5
OU6

FIG. 2

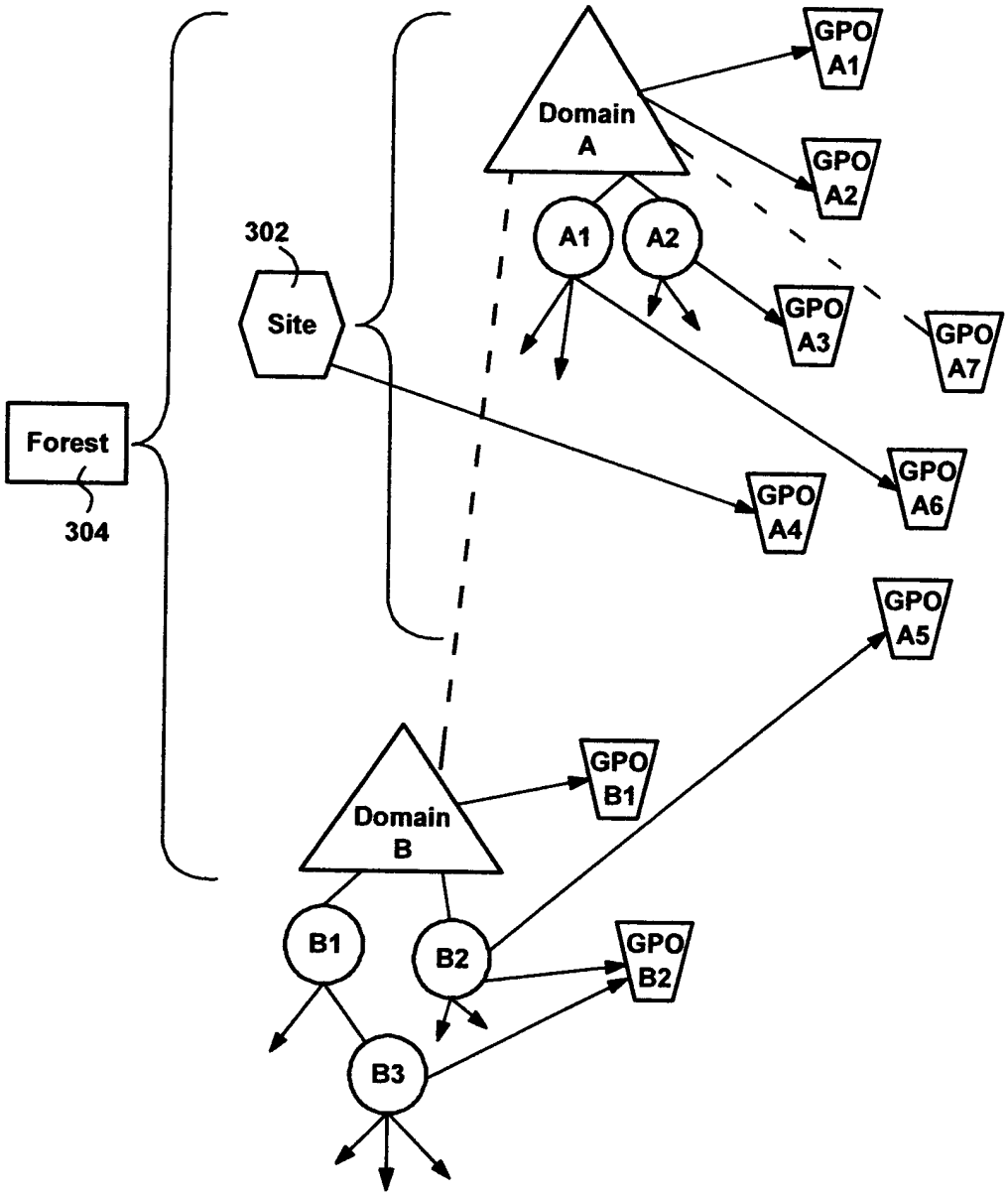

Forest
304
302
Site
Domain
A
A1
A2
GPO
A1
GPO
A2
GPO
A3
GPO
A7
GPO
A4
GPO
A6
GPO
A5
Domain
B
B1
B2
B3
GPO
B1
GPO
B2

FIG. 3

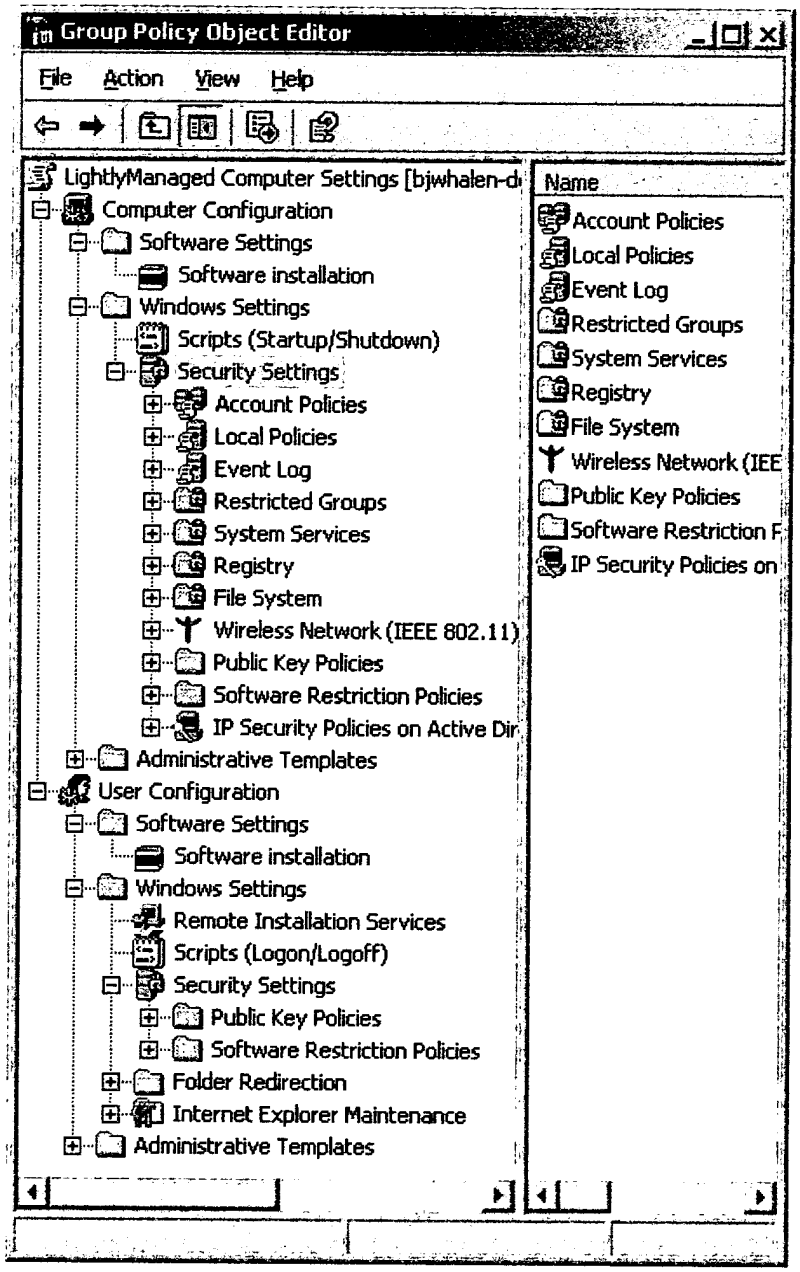


FIG. 4
Prior art

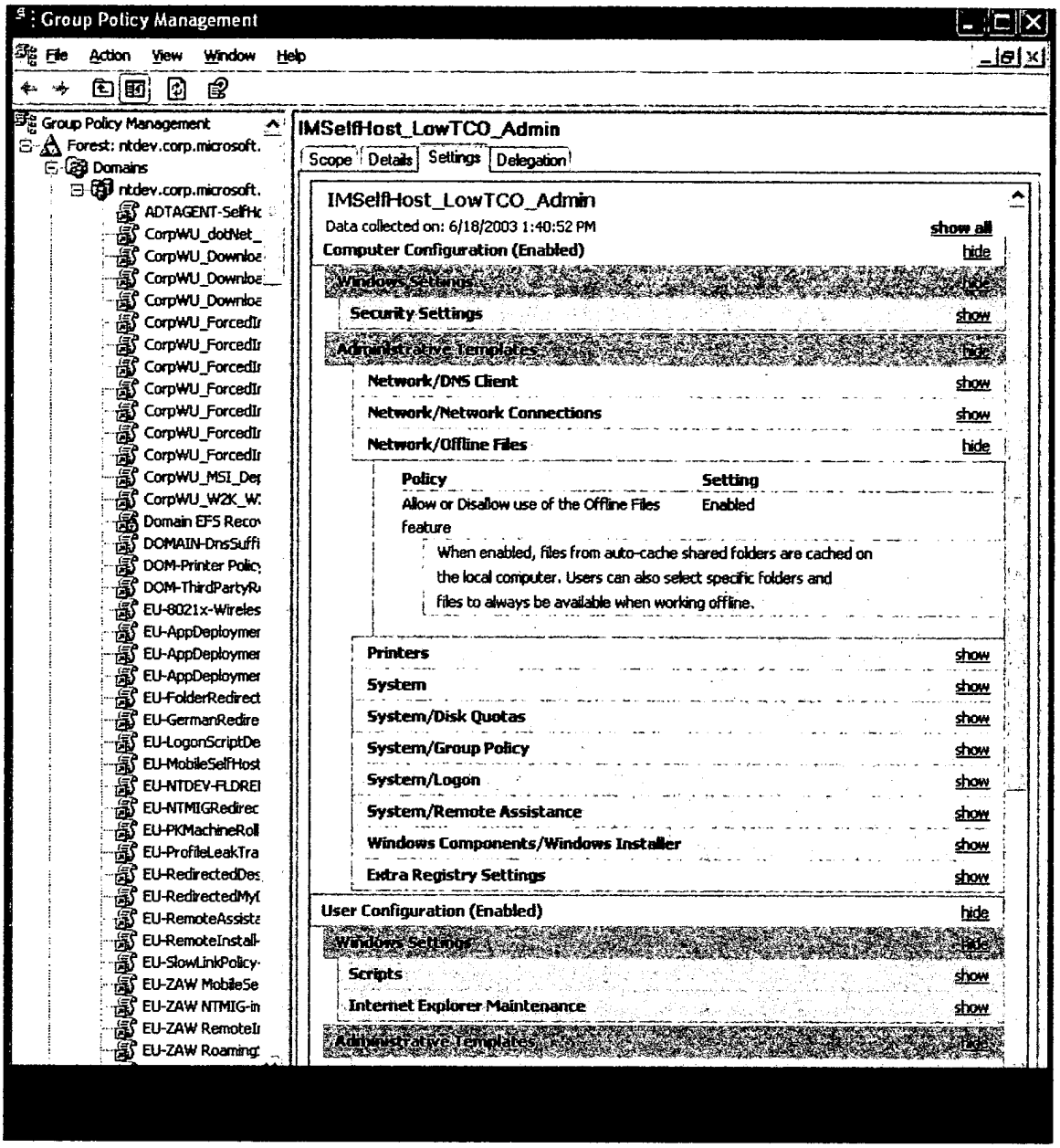
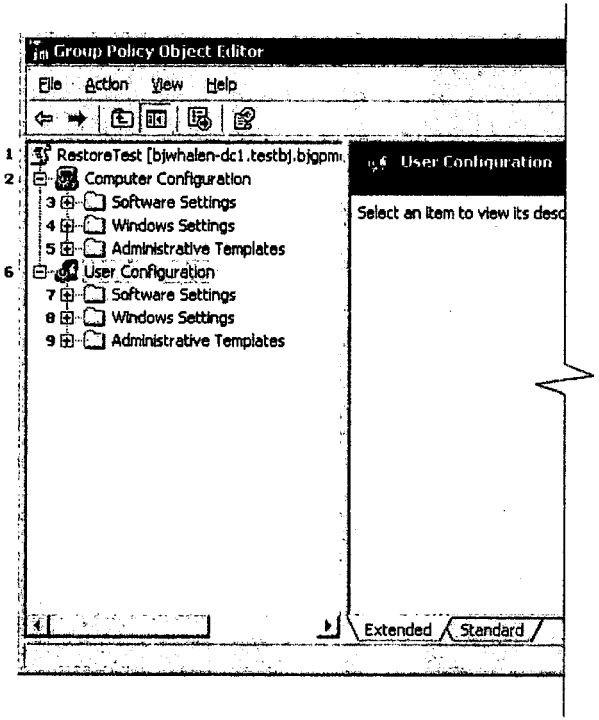

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: ntdev.corp.microsoft.
Domains
ntdev.corp.microsoft.
ADTAGENT-SelfHc
CorpWU_dotNet_
CorpWU_Downloa
CorpWU_Downloa
CorpWU_Downloa
CorpWU_ForcedIr
CorpWU_ForcedIr
CorpWU_ForcedIr
CorpWU_ForcedIr
CorpWU_ForcedIr
CorpWU_ForcedIr
CorpWU_ForcedIr
CorpWU_MSI_Dep
CorpWU_W2K_W
Domain EFS Reco
DOMAIN-DnsSuffi
DOM-Printer Policy
DOM-ThirdPartyRu
EU-8021x-Wireles
EU-AppDeploymer
EU-AppDeploymer
EU-AppDeploymer
EU-FolderRedirect
EU-GermanRedire
EU-LogonScriptDe
EU-MobileSelfHost
EU-NTDEV-FLDREI
EU-NTMIGRedirec
EU-PKMachineRoll
EU-ProfileLeakTra
EU-RedirectedDes
EU-RedirectedMyI
EU-RemoteAssista
EU-RemoteInstall-
EU-SlowLinkPolicy-
EU-ZAW MobileSe
EU-ZAW NTMIG-in
EU-ZAW RemoteIr
EU-ZAW Roaming
IMSelfHost_LowTCO_Admin
Scope Details Settings Delegation
IMSelfHost_LowTCO_Admin
Data collected on: 6/18/2003 1:40:52 PM
show all
Computer Configuration (Enabled)
hide
Windows Settings
hide
Security Settings
show
Administrative Templates
hide
Network/DNS Client
show
Network/Network Connections
show
Network/Offline Files
hide
Policy
Setting
Allow or Disallow use of the Offline Files feature
Enabled
When enabled, files from auto-cache shared folders are cached on the local computer. Users can also select specific folders and files to always be available when working offline.
Printers
show
System
show
System/Disk Quotas
show
System/Group Policy
show
System/Logon
show
System/Remote Assistance
show
Windows Components/Windows Installer
show
Extra Registry Settings
show
User Configuration (Enabled)
hide
Windows Settings
hide
Scripts
show
Internet Explorer Maintenance
show
Administrative Templates
hide

FIG. 5

Tree to Report Mapping

Highest Level (consistent) buckets



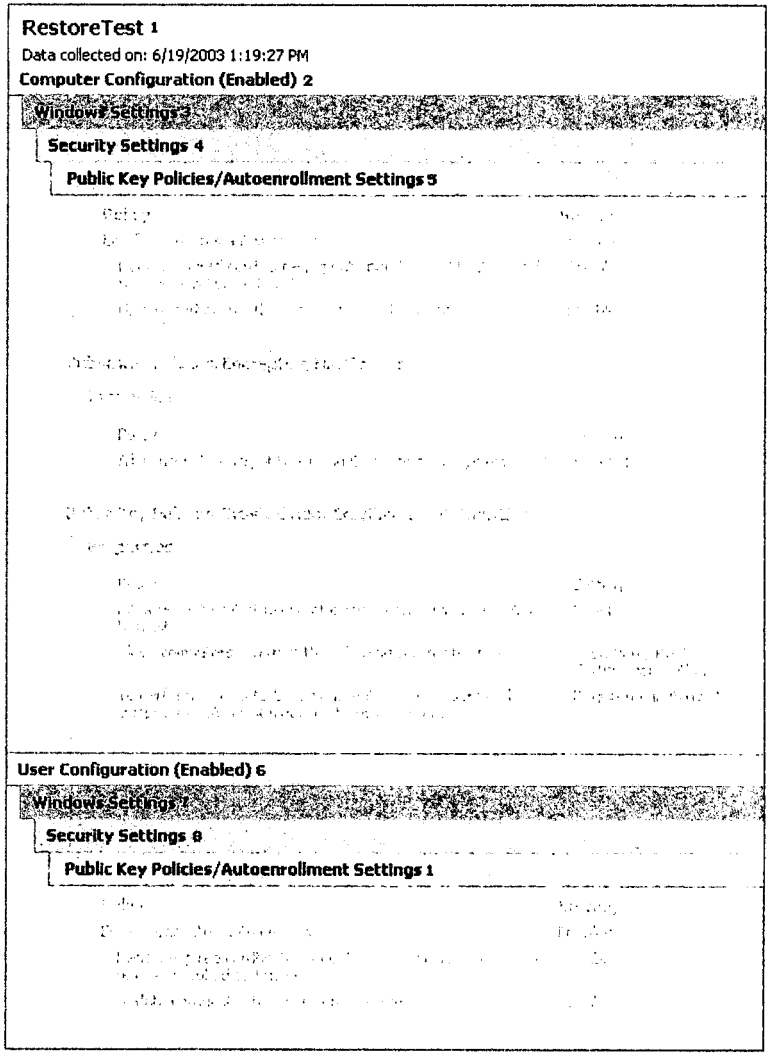


FIG. 6

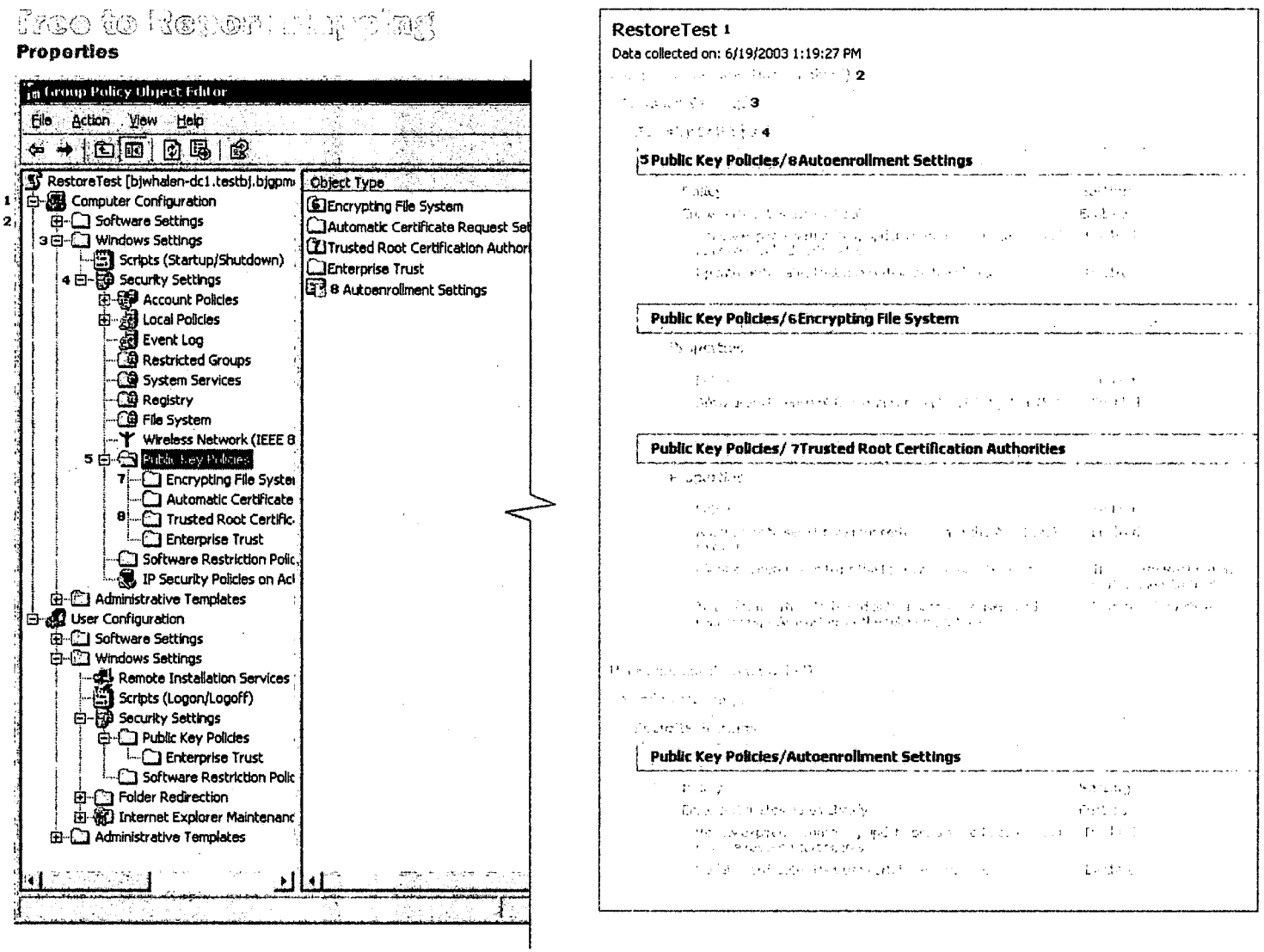

Properties
Group Policy Object Editor
File Action View Help
RestoreTest [bjwhalen-dc1.testbj.bjgpm
Computer Configuration
Software Settings
Windows Settings
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wireless Network (IEEE 8
Public Key Policies
Encrypting File Syste
Automatic Certificate
Trusted Root Certific
Enterprise Trust
Software Restriction Polic
IP Security Policies on Acl
Administrative Templates
User Configuration
Software Settings
Windows Settings
Remote Installation Services
Scripts (Logon/Logoff)
Security Settings
Public Key Policies
Enterprise Trust
Software Restriction Polic
Folder Redirection
Internet Explorer Maintenanc
Administrative Templates
Object Type
Encrypting File System
Automatic Certificate Request Set
Trusted Root Certification Author
Enterprise Trust
Autoenrollment Settings
RestoreTest 1
Data collected on: 6/19/2003 1:19:27 PM
Public Key Policies/Autoenrollment Settings
Public Key Policies/Encrypting File System
Public Key Policies/Trusted Root Certification Authorities
Public Key Policies/Autoenrollment Settings

FIG. 7

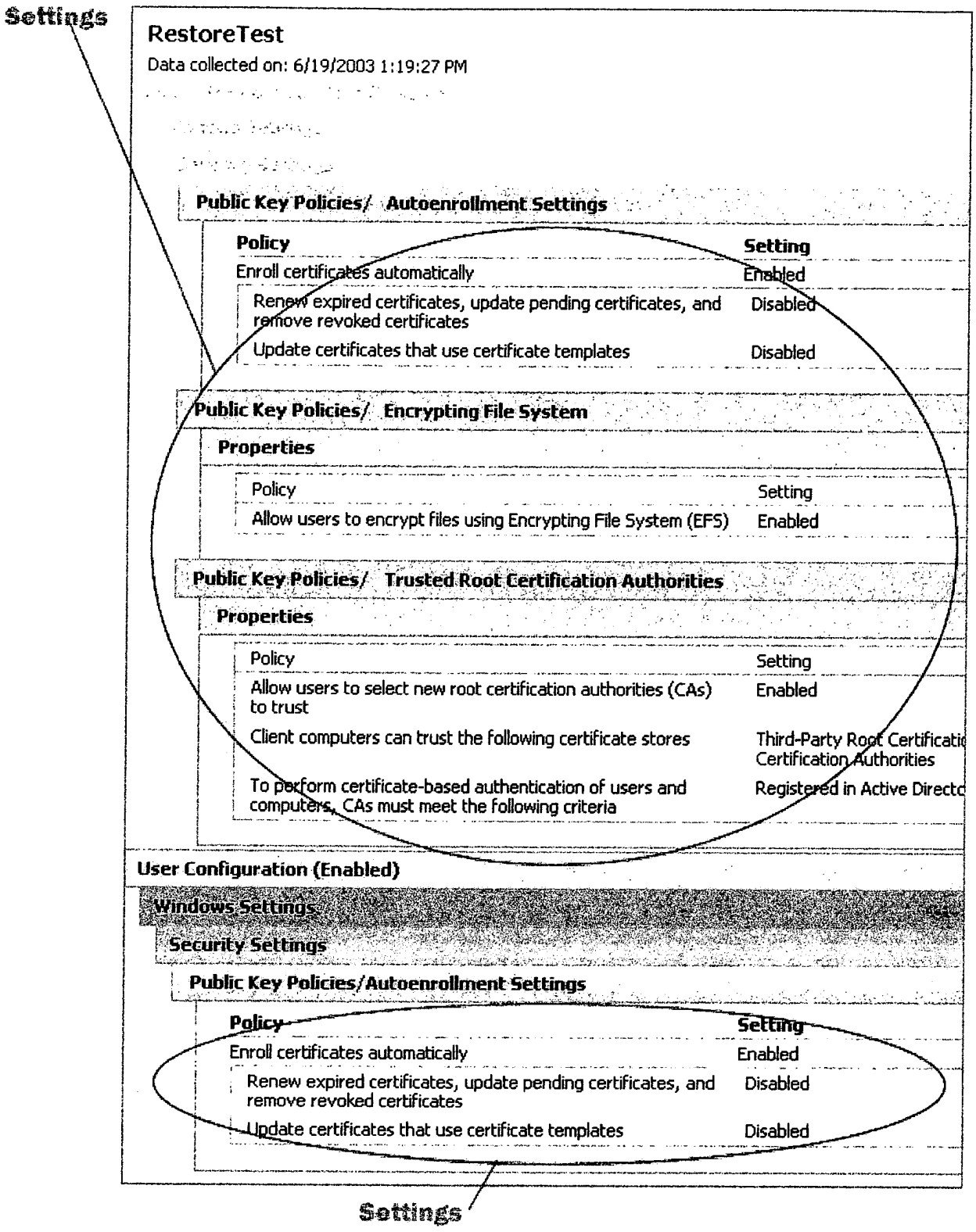
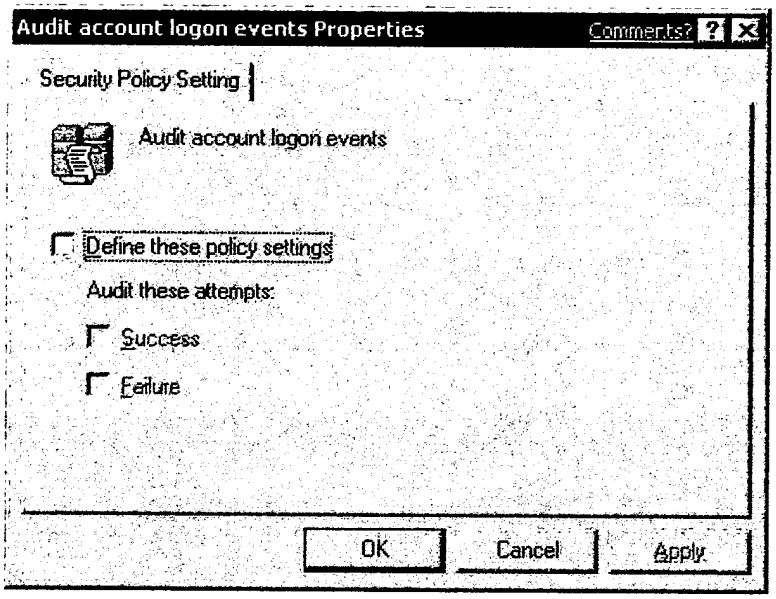
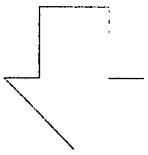

Settings
RestoreTest
Data collected on: 6/19/2003 1:19:27 PM
Public Key Policies/ Autoenrollment Settings
Policy
Setting
Enroll certificates automatically
Enabled
Renew expired certificates, update pending certificates, and remove revoked certificates
Disabled
Update certificates that use certificate templates
Disabled
Public Key Policies/ Encrypting File System
Properties
Policy
Setting
Allow users to encrypt files using Encrypting File System (EFS)
Enabled
Public Key Policies/ Trusted Root Certification Authorities
Properties
Policy
Setting
Allow users to select new root certification authorities (CAs) to trust
Enabled
Client computers can trust the following certificate stores
Third-Party Root Certificati
Certification Authorities
To perform certificate-based authentication of users and computers, CAs must meet the following criteria
Registered in Active Directc
User Configuration (Enabled)
Windows Settings
Security Settings
Public Key Policies/Autoenrollment Settings
Policy
Setting
Enroll certificates automatically
Enabled
Renew expired certificates, update pending certificates, and remove revoked certificates
Disabled
Update certificates that use certificate templates
Disabled
Settings

FIG. 8





Local Policies/Audit Policy	
Policy	**Setting**
Audit account logon events	Success

FIG. 9

Local Policies/Audit Policy

Policy	Setting
Audit account logon events	Success
Audit account management	No auditing
Audit directory service access	No auditing

FIG. 10

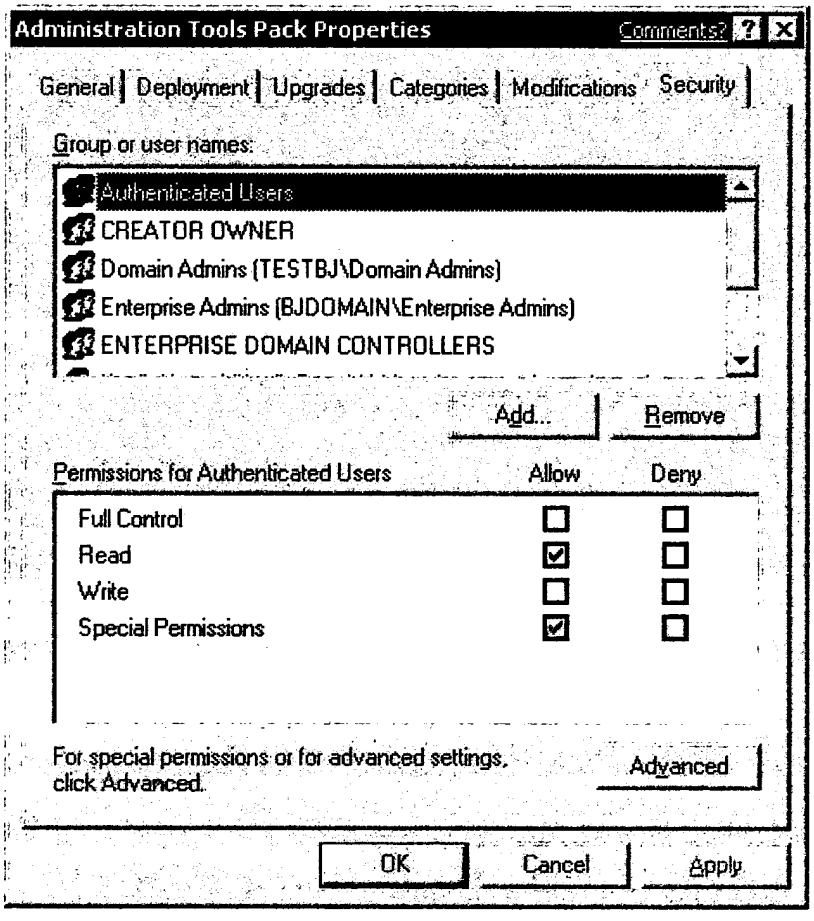
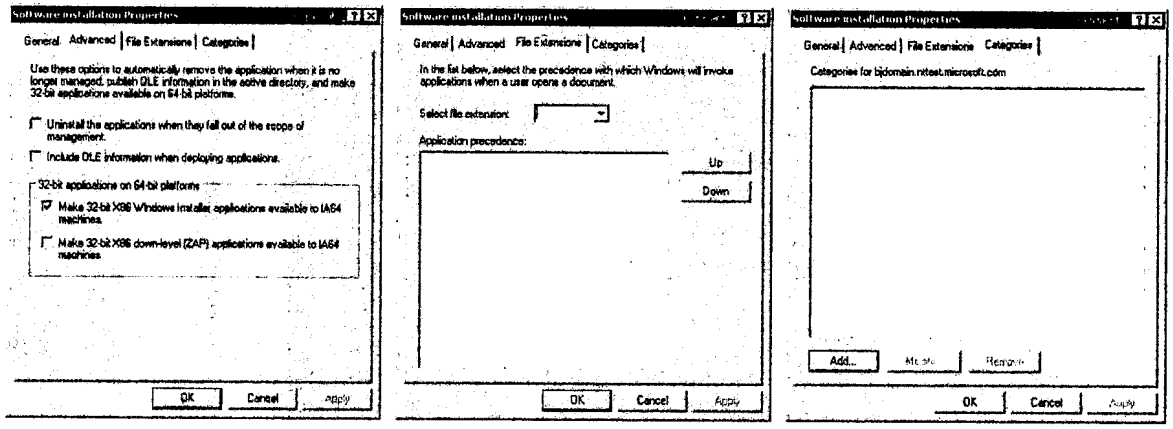


FIG. 12
Prior Art



Software Installation	
General	
Policy	**Security Setting**
Add data here	10 minutes
Advanced	
Policy	**Security Setting**
Add data here	COMCFG; DFS$
File Extensions	
Policy	**Security Setting**
Add data here	COMCFG; DFS$
Categories	
Policy	**Security Setting**
Add data here	Enabled

FIG. 11

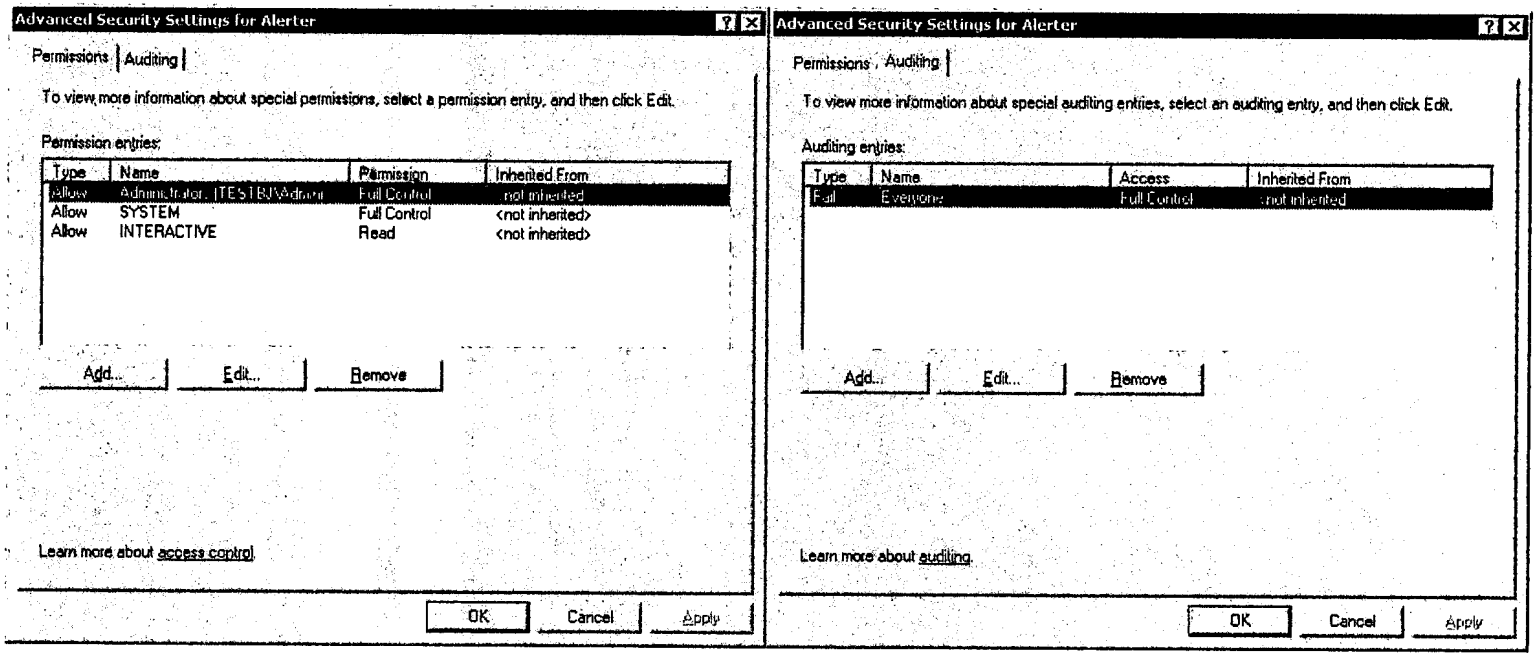


FIG. 13
Prior Art

Local Policies/Security Options

Microsoft network server

Policy	Security Setting
Amount of idle time required before suspending session	10 minutes

Network access

Policy	Security Setting
Network access: Shares hat can be accessed anonymously	COMCFG; DFS$

Network security

Policy	Security Setting
Minimum session security for NTLM SSP based (including secure RPC clients)	Enabled
Require message integrity	Enabled
Require message confidentiality	Disabled
Require NTLMv@ session security	Disabled
Require 128-bit encryption	Disabled
Minimum session security for NTLM SSP based (including secure RPC servers)	Enabled
Require message integrity	Enabled
Require message confidentiality	Disabled
Require NTLMv@ session security	Disabled
Require 128-bit encryption	Disabled

System objects: Strengthen default permissions of internal system objects

Policy	Security Setting
Strengthen default permissions of internal system objects	Enabled

System objects

Policy	Security Setting
Default owner for objects created by members of Administrators group	Adminstrators Group

FIG. 14

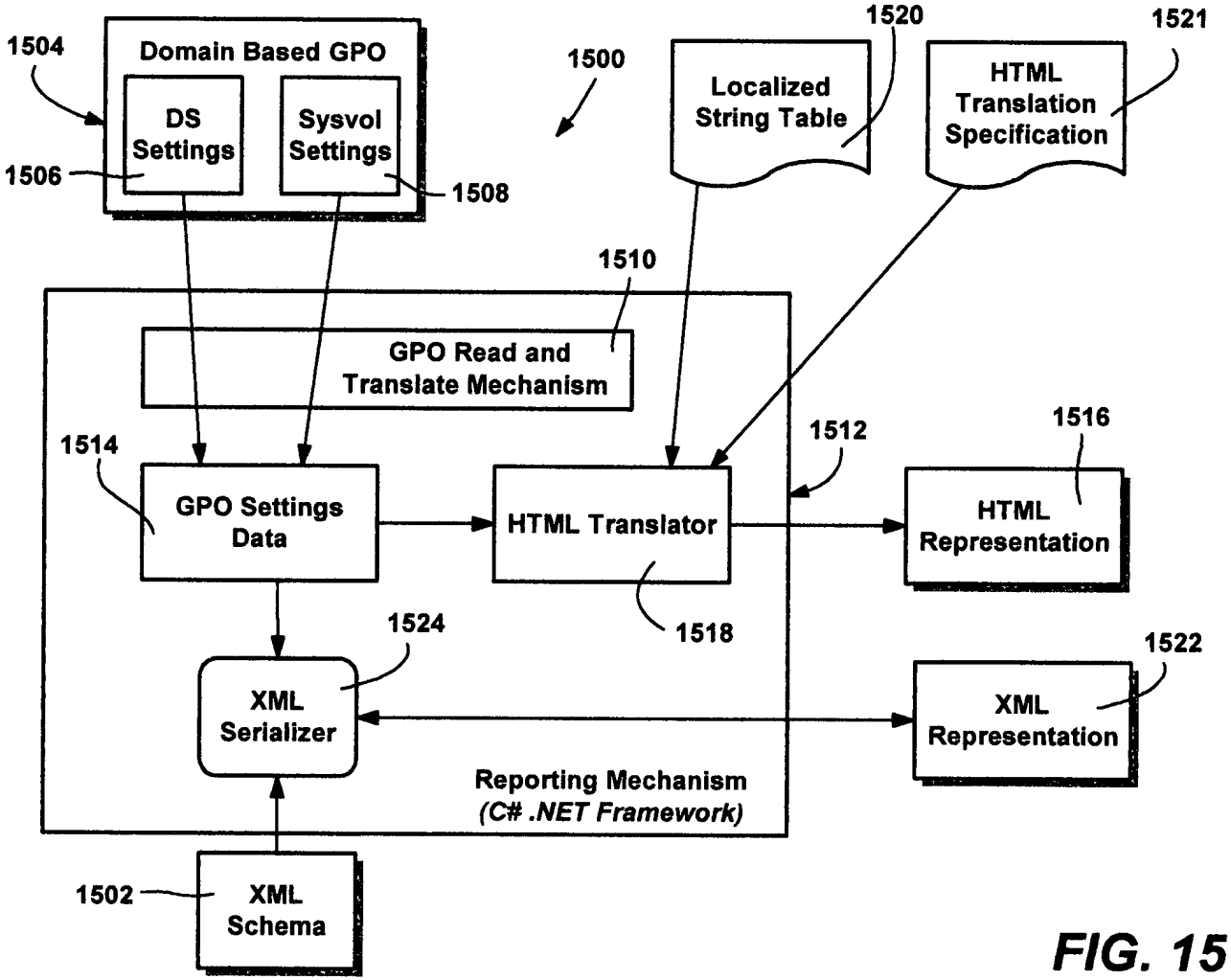

1504
Domain Based GPO
DS Settings
Sysvol Settings
1506
1508
1500
1520
Localized String Table
1521
HTML Translation Specification
1510
GPO Read and Translate Mechanism
1514
GPO Settings Data
HTML Translator
1512
1516
HTML Representation
1518
1524
XML Serializer
1522
XML Representation
Reporting Mechanism
(C# .NET Framework)
1502
XML Schema

FIG. 15

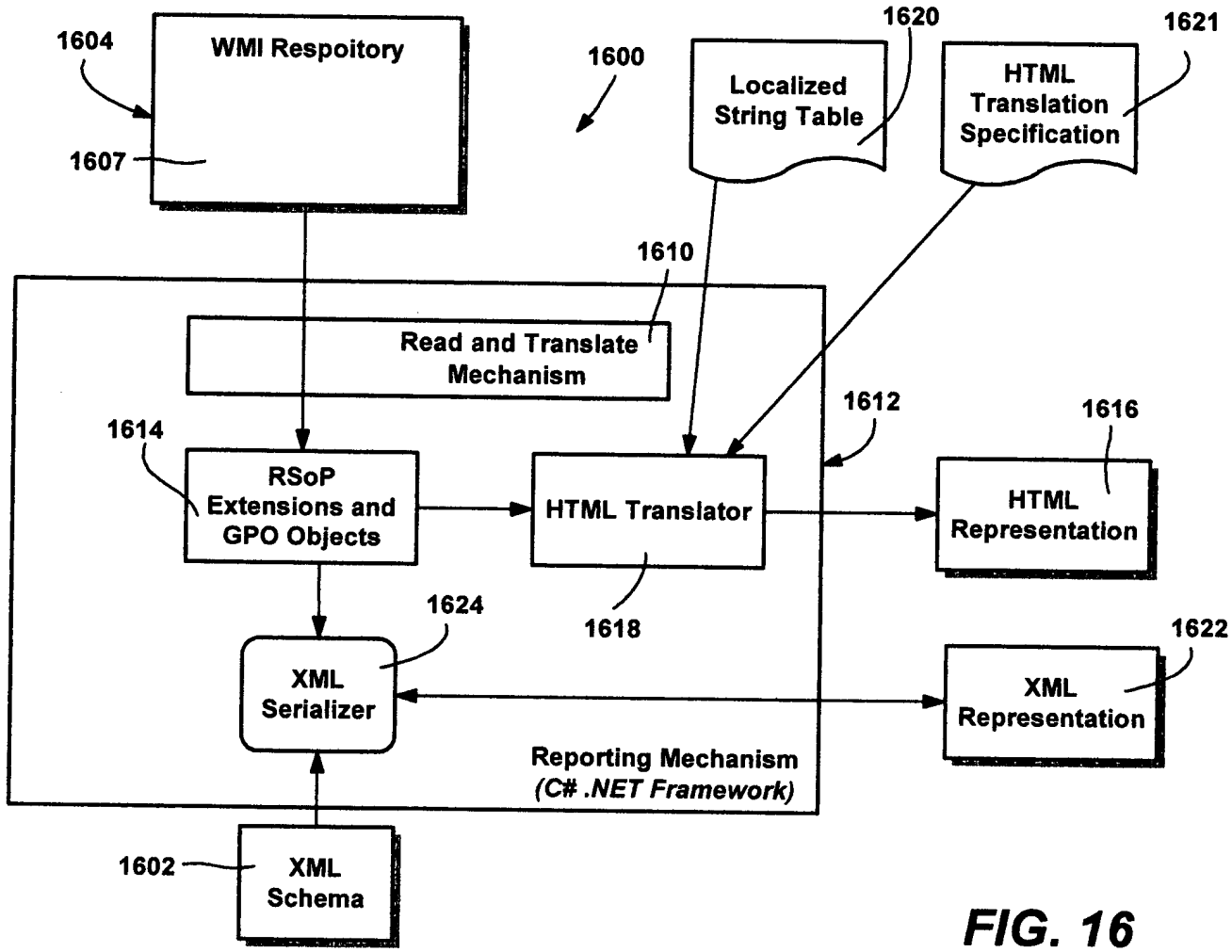

1604
WMI Respoitory
1607
1600
1620
Localized String Table
1621
HTML Translation Specification
1610
Read and Translate Mechanism
1612
1614
RSoP Extensions and GPO Objects
HTML Translator
1616
HTML Representation
1618
1624
XML Serializer
1622
XML Representation
Reporting Mechanism
(C# .NET Framework)
1602
XML Schema

FIG. 16

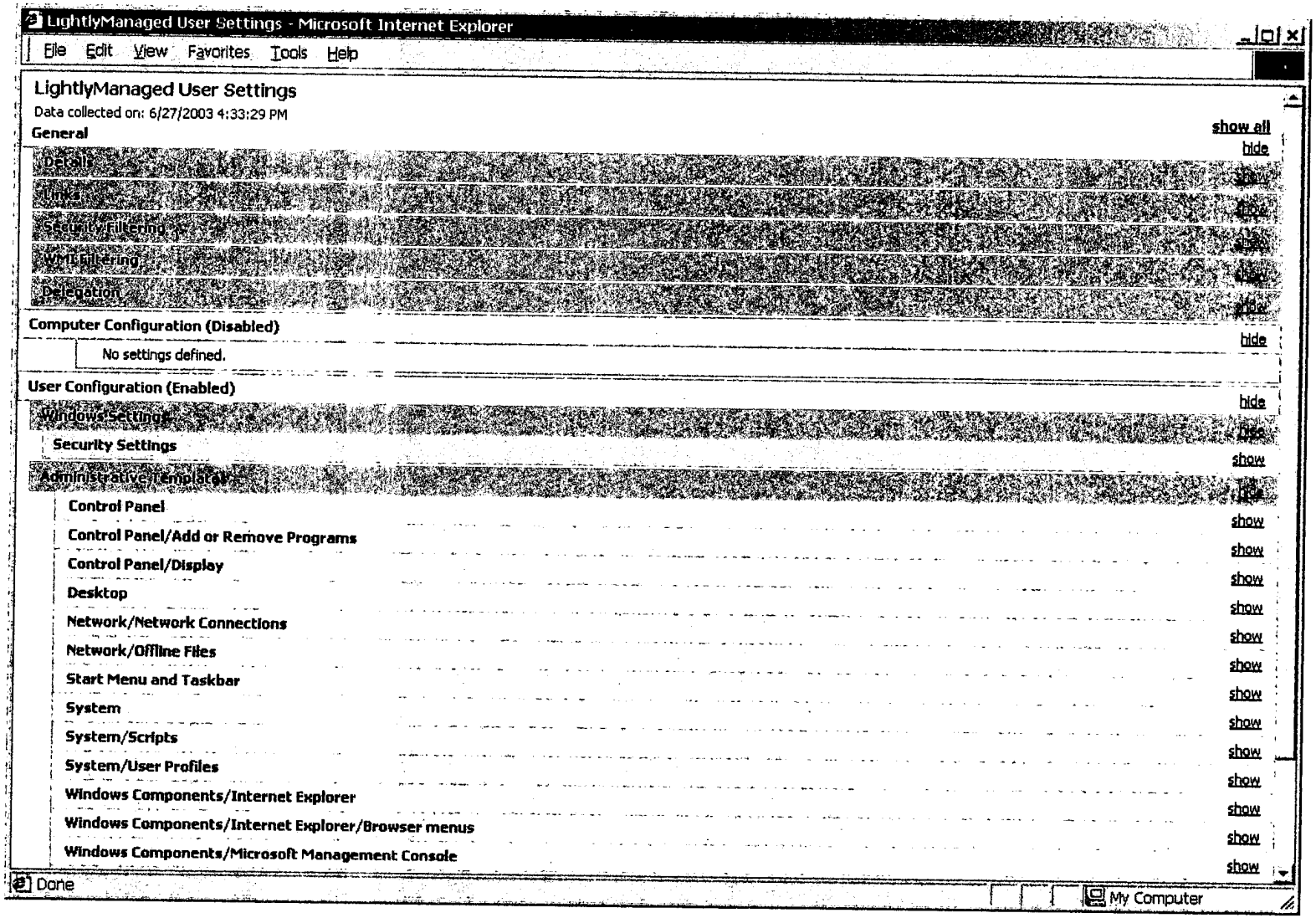

LightlyManaged User Settings - Microsoft Internet Explorer
File Edit View Favorites Tools Help
LightlyManaged User Settings
Data collected on: 6/27/2003 4:33:29 PM
General
show all
hide
Details
Links
Security Filtering
WMI filtering
Delegation
Computer Configuration (Disabled)
hide
No settings defined.
User Configuration (Enabled)
hide
Windows Settings
Security Settings
show
Administrative Templates
Control Panel
Control Panel/Add or Remove Programs
Control Panel/Display
Desktop
Network/Network Connections
Network/Offline Files
Start Menu and Taskbar
System
System/Scripts
System/User Profiles
Windows Components/Internet Explorer
Windows Components/Internet Explorer/Browser menus
Windows Components/Microsoft Management Console
Done
My Computer

FIG. 17

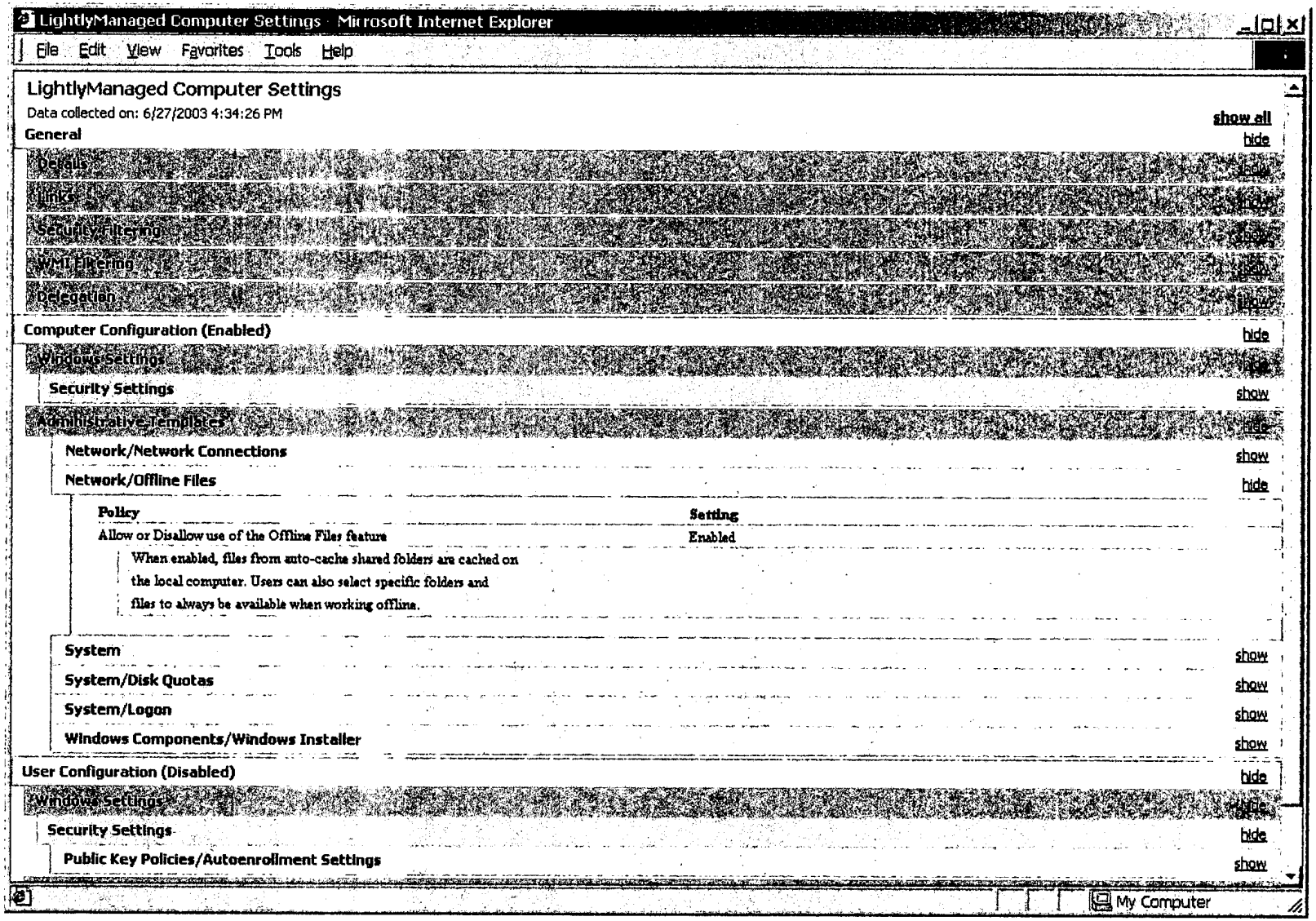

LightlyManaged Computer Settings - Microsoft Internet Explorer
File Edit View Favorites Tools Help
LightlyManaged Computer Settings
Data collected on: 6/27/2003 4:34:26 PM
show all
General
hide
Details
show
Links
show
Security Filtering
show
WMI Filtering
show
Delegation
show
Computer Configuration (Enabled)
hide
Windows Settings
hide
Security Settings
show
Administrative Templates
hide
Network/Network Connections
show
Network/Offline Files
hide
Policy
Setting
Allow or Disallow use of the Offline Files feature
Enabled
When enabled, files from auto-cache shared folders are cached on the local computer. Users can also select specific folders and files to always be available when working offline.
System
show
System/Disk Quotas
show
System/Logon
show
Windows Components/Windows Installer
show
User Configuration (Disabled)
hide
Windows Settings
hide
Security Settings
hide
Public Key Policies/Autoenrollment Settings
show
My Computer

FIG. 18

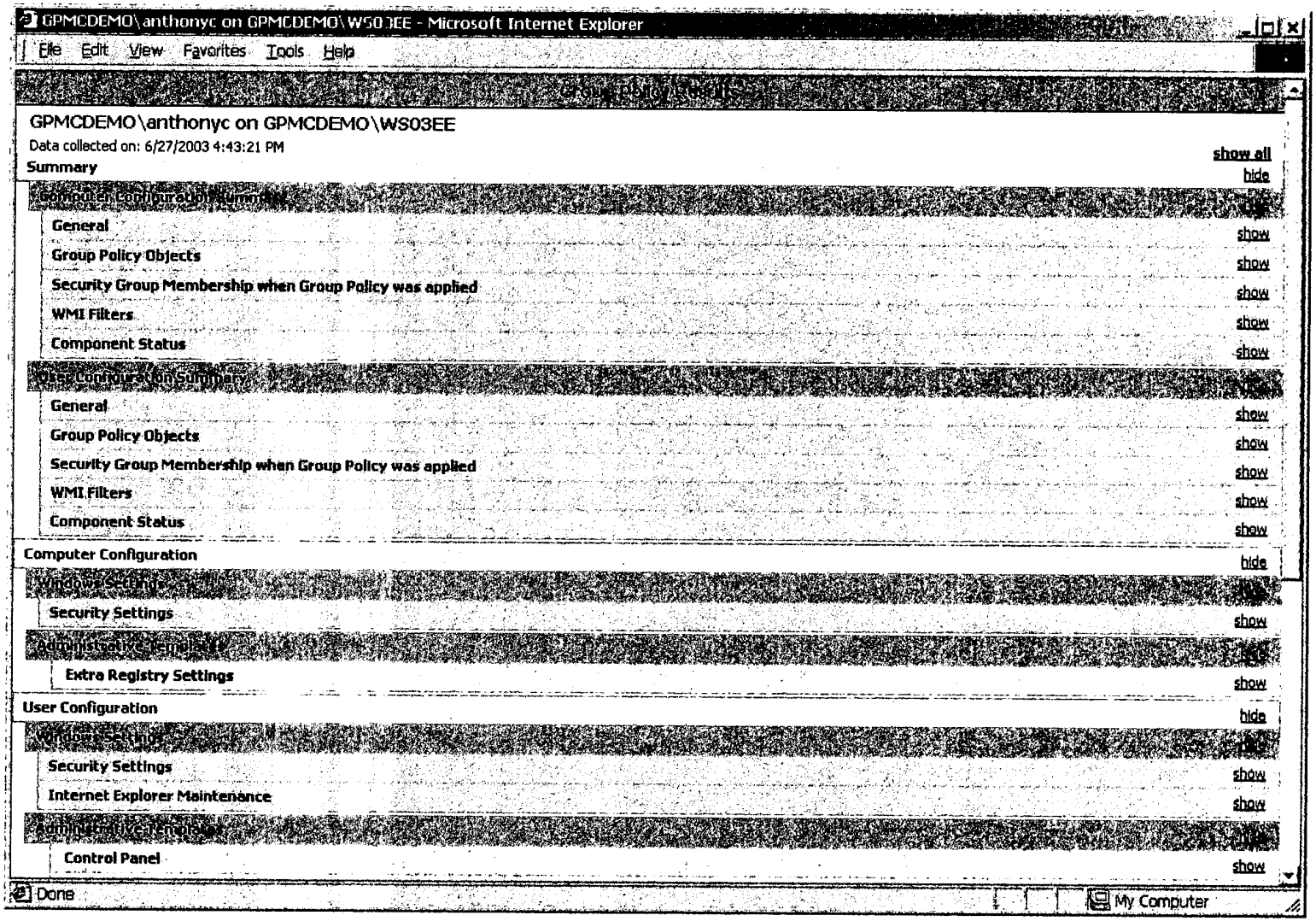

GPMCDEMO\anthonyc on GPMCDEMO\WS03EE - Microsoft Internet Explorer
File Edit View Favorites Tools Help
GPMCDEMO\anthonyc on GPMCDEMO\WS03EE
Data collected on: 6/27/2003 4:43:21 PM
Summary
show all
hide
General
Group Policy Objects
Security Group Membership when Group Policy was applied
WMI Filters
Component Status
User Configuration Summary
General
Group Policy Objects
Security Group Membership when Group Policy was applied
WMI Filters
Component Status
Computer Configuration
hide
Windows Settings
Security Settings
Administrative Templates
Extra Registry Settings
User Configuration
hide
Windows Settings
Security Settings
Internet Explorer Maintenance
Administrative Templates
Control Panel
show
Done
My Computer

FIG. 19